What is claimed is:

1. A method for identification, detection and investigation of maleficent acts, comprising the steps of:

receiving one or more transaction datasets;

verifying each transaction dataset identity and classifying each transaction dataset into a first category, a second category and a third category;

detecting and arbitrating ambiguities in each transaction dataset in the second category for reclassifying into the first category and the third category;

investigating each transaction dataset in the third category for affirming the third category classification of a first group of investigated datasets and reclassifying the third category classification of a remaining second group of investigated datasets into the first category classification;

enabling transaction datasets in the first category; and

disabling transaction datasets in the third category.

2. The method of claim 1, wherein the step of receiving one or more transaction datasets further comprises receiving one or more transaction datasets selected from the group consisting of airline reservations, cargo transactions, border crossings, Patriot Act transactions, insurance claims, underwriting insurance transactions, and credit applications.

3. The method of claim 1, wherein the step of verifying and classifying further comprises verifying each transaction dataset identity by assigning a composite score to each transaction dataset and classifying each transaction dataset by assigning each dataset to the predetermined categories according to each dataset composite score.

4. The method of claim 3, wherein the composite score assigned to each transaction dataset is determined by combining one or more analytical scores based on a comparison between each transaction dataset and one or more similar datasets located in disparate databases.

5. The method of claim 4, wherein a means for determining the one or more analytical scores is selected from the group consisting of a similarity search engine, a biometric analytic, a rules engine, and a neural net.

6. The method of claim 3, further comprising the step of assigning a composite score to each transaction dataset according to a schema defined by a user.

7. The method of claim 6, further comprising designating an analytic function in the schema selected from the group consisting of a similarity search function, a biometric function, a rules function, and a neural net function.

8. The method of claim 1, wherein the step of classifying datasets into categories is determined by preset classes, business rules and associations determined by a user to meet specific business needs.

9. The method of claim 1, further comprising the step of controlling and monitoring a workflow process comprising the steps of receiving, verifying and classifying, detecting and arbitrating, investigating, enabling and disabling.

10. The method of claim 1, wherein the step of detecting and arbitrating ambiguities comprises the steps of:

receiving transaction datasets classified into the second category in the verifying step;

enabling an arbitrator to view a summary list screen showing transaction dataset identification, classification, status, justification, and links to a transaction dataset detail screen, a search form screen, and a search queue screen;

enabling the arbitrator to view a task detail screen for comparing analytical scores between selected transaction datasets and datasets contained in disparate databases; and

enabling the arbitrator to change the classification of transaction datasets from the second category into a category selected from the group consisting of the first category and the third category.

11. The method of claim 10, further comprising enabling the arbitrator to select an analytic function for determining a comparative analytical score of a selected transaction dataset, the analytic function selected from the group consisting of a similarity search function, a biometric function, a rules function, a neural net function, a model engine and a decision tree.

12. The method of claim 10, further comprising enabling the arbitrator to update a classification and status of selected transaction datasets.

13. The method of claim 1, wherein the step of investigating each transaction dataset in the third category comprises the steps of:

receiving transaction datasets classified into the third category in the steps of verifying and detecting;

enabling an investigator to view a summary list screen showing transaction datasets containing links to a task detail screen, a search form screen, and a search queue screen;

enabling the investigator to view a task detail screen for comparing elements of a selected transaction dataset to elements from comparison datasets contained in disparate databases; and

enabling the investigator to change the classification of transaction datasets from the second category into the first category and the third category.

14. The method of claim 13, further comprising enabling the investigator to select an analytic function for determining a comparative analytical score of a selected transaction dataset, the analytic function selected from the group consisting of a similarity search function, a biometric function, a rules engine, a neural net, a model engine, an auto link analysis, a decision tree, and a report engine.

15. The method of claim 1, further comprising activating remote similarity search agents in disparate databases to be searched by a similarity search function, the remote similarity search agents returning similarity scores and results to the similarity search function without a requirement for relocating the searched information from the disparate databases.

16. A computer-readable medium containing instructions for controlling a computer system according to the method of claim 1.

17. A system for identification, detection and investigation of maleficent acts, comprising:

a means for receiving one or more transaction datasets;

a means for verifying each transaction dataset identity and classifying each transaction dataset into a first category, a second category and a third category;

a means for detecting and arbitrating ambiguities in each transaction dataset in the second category for reclassifying into the first category and the third category;

a means for investigating each transaction dataset in the third category for affirming the third category classification of a first group of investigated datasets and reclassifying the third category classification of a remaining second group of investigated datasets into the first category classification;

a means for enabling transaction datasets in the first category; and

a means for disabling transaction datasets in the third category.

18. The system of claim 17, wherein:

the means for receiving and the means for verifying and classifying comprise a classification engine;

the means for detecting and arbitrating comprise an arbitration function; and

the means for investigating comprise an investigation function.

19. The system of claim 17, further comprising a workflow manager for controlling and monitoring a workflow process comprising the means for of receiving, verifying and classifying, detecting and arbitrating, investigating, enabling and disabling.

20. The system of claim 18, wherein the classification engine, the arbitration function and the investigation function have access to disparate databases through analytic functions.

21. The system of claim 20, wherein the disparate databases comprise an alias identification database, an expert rules database, a government threat database, public databases, and known threat databases.

22. The system of claim 21, wherein the disparate databases contain remote similarity search agents for returning similarity scores and results to the similarity search engine

without a requirement for relocating the searched information from the disparate databases.

23. The system of claim 21, wherein the analytic functions comprise a similarity search function, a biometric function, a rules engine, a neural net, a model engine, an auto link analysis, a decision tree, and a report engine.

24. The system of claim 19, wherein the arbitration function includes a user interface for enabling a user to arbitrate the second category classification decisions made by the classification engine into the first and third category classification.

25. The system of claim 19, wherein the investigation function includes a user interface for enabling a user to investigate the third category classification decisions made by the classification engine and the arbitration function and to reassign them to the first and the third category classification.

26. A method for identification, detection and investigation of maleficent acts, comprising the steps of:

controlling a workflow process for classifying transaction datasets into a high risk category and a low risk category, including the steps of:

verifying and classifying transaction datasets;

detecting and arbitrating transaction dataset ambiguities;

investigating high risk transaction datasets for ensuring correct classification;

initiating analytic functions comprising a similarity search function, a biometric function, a rules engine, a neural net, a model engine, an auto link analysis, a decision tree, and a report engine; and accessing disparate databases including an alias identification database, an expert rules database, a government threat database, public databases, and known threat databases.

27. The method of claim 26, wherein the disparate databases contain remote similarity search agents for returning similarity scores and results to the similarity search engine without a requirement for relocating the searched information from the disparate databases.